Ms. Isabelle Falque-Pierrotin
Chairman, Article 29 Working Party

MEP Claude Moraes
Chair of the Committee on Civil Liberties, Justice, and Home Affairs

HE Pieter de Gooijer
Ambassador and Permanent Representative of the Netherlands to the EU

cc: Secretary Penny Pritzker
Commissioner Věra Jourová

March 16, 2016

Ms. Falque-Pierrotin, MEP Moraes, and Ambassador de Gooijer,

We, the undersigned organizations do not believe that the Privacy Shield arrangement between the United States and the European Union complies with the standards set by the Court of Justice of the European Union (CJEU), including in the recent case invalidating the legal underpinnings of the Safe Harbor Framework.[1] Without more substantial reforms to ensure protection for fundamental rights of individuals on both sides of the Atlantic, the Privacy Shield will put users at risk, undermine trust in the digital economy, and perpetuate the human rights violations that are already occurring as a result of surveillance programs and other activities.

The Article 29 Working Party thoughtfully outlined four key conditions for an agreement to meet the standards of European legislation and guarantee the protection of human rights in intelligence activity, including clarity of law, use of human rights standards, incorporation of independent oversight, and availability of effective remedy.[2] Unfortunately, the Privacy Shield manifestly fails to provide for these objectives.[3]

While questions remain about the scope and utility of certain provisions of the Privacy Shield,[4] it is beyond doubt that the continued existence of the same inadequacies in US law

[1] C-362/14, Maximilian Schrems v Data Protection Commissioner, 2015 http://curia.europa.eu (Oct.6, 2015), http://curia.europa.eu/juris/document/document.jsftext=&docid=169195&pageIndex=0&doclang=EN&mode=req.

[2] Statement of the Article 29 Working Party on the Consequences of the Schrems Judgment (Feb. 3, 2016) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf.

[3] *See, e.g.,* Netzwerk Datenschutzexpertise (Data Protection Expertise Network), *Privacy Shield – Darstellung und rechtliche Bewertung,* http://www.netzwerk-datenschutzexpertise.de.

[4] For example, what level of redress does the proposed Alternative Dispute Mechanism offer as compared to independent judicial oversight? Are the exemptions from the opt-in system proportionate? What is the legal status of the written assurances provided by the intelligence community? What limits are placed on the collection of EU data by the intelligence community? Have the EU and US reached a common understanding on the definitions of key surveillance terms, like "bulk surveillance"?

that existed at the time of the CJEU's judgment mean EU citizens still cannot be sure what will happen to their data once transferred to the US. Specifically, the US government continues to deny the relevance and application of the internationally-accepted standards of necessity and proportionality in its surveillance operations. In addition, the oversight mechanism established by the Privacy Shield to respond to complaints about US surveillance is not independent, nor does the office come empowered with sufficient authority to initiate investigations or respond adequately to complaints.[5] Finally, due to the fact that individuals are never notified when their information has been collected, disseminated, or used, any remedy for individuals will be unavailable for all practical purposes.

In order for the Privacy Shield to survive, the US must formally commit to substantial reforms to respect human rights and international law in order to meet the standards set forth by the CJEU and the Article 29 Working Group.[6] The Privacy Shield contains no such commitment.

The Privacy Shield should be contingent on US legislative reform of surveillance laws within a reasonable time. These reforms must include, at a minimum, the incorporation of human rights standards (applying to both US persons and non-US persons), a narrowed definition of "foreign intelligence information" to limit the scope of data collection, and more limited access to, retention of, and use of data after it is collected. Indiscriminate scanning of communications content and metadata, specifically, must be discontinued.

In addition to surveillance reform, a lasting data transfer framework requires increased protections for personal data collected or used commercially in order to meet the standards set forth by the CJEU. Wider data protection reforms, which must include robust and comprehensive enforcement mechanisms, are necessary to ensure that the US provides a level of essentially equivalent protection to that available under the European legal framework.

Finally, the Privacy Shield must include provisions to ensure appropriate redress and transparency.

In recognition of the changes needed in order to build a solid foundation for mutual trust across the Atlantic, we urge you to send the Privacy Shield back to the negotiators for further consideration in order to address the identified issues. These reforms and

---

[5] Emily O'Reilly, Use of the title 'ombudsman' in the 'EU-US Privacy Shield" agreement, European Ombudsman (Febr. 22, 2016), http://www.ombudsman.europa.eu/resources/otherdocument.faces/en/64157/html.bookmark. When reviewing complaints, the Ombudsperson only ensures that data was handled appropriately under existing US law and policy, which lack adequate data protections. Even in cases where the Ombudsperson does find that data was handled improperly, she will neither confirm nor deny that the complainant was the target of surveillance, nor will she inform the individual of the specific remedial action taken. And, the Ombudsperson will not respond to any general claims that the agreement is inconsistent with EU data protection laws.

[6] To prevent a double standard, the Commission must seek a similar pledge from EU Member States to commit to reforming their surveillance authorities.

safeguards would help protect individuals' human rights and provide the legal certainty needed by companies operating trans-nationally.

Sincerely,

Access Now
Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee (ADC)
American Civil Liberties Union (ACLU)
Amnesty International USA
Association for Technology and Internet (APTI)
Bits of Freedom
Center for Digital Democracy
Consumer Action
Consumer Federation of America
Consumer Watchdog
Cyber Privacy Project
Defending Dissent/Bill of Rights Defense Committee
Digitale Gesellschaft e.V.
Digital Rights Ireland
Electronic Frontier Foundation
Electronic Privacy Information Center
European Digital Rights (EDRi)
Fight for the Future
IT-Political Association of Denmark
Panoptykon Foundation
Patient Privacy Rights
Privacy International
Privacy Rights Clearinghouse
La Quadrature du Net
Restore the Fourth
X-Lab